Computer User's Security Guide

This Computer User's Security Guide is an integral part of the state's security information management program. You, the employee, therefore are a key factor in protecting information, as you use it in your daily job. The intent of this guide is to educate you on information security by making you aware of threats and risks, giving you a good set of rules to incorporate into your own business practices, and to know what to do if you encounter a security violation.

Witnessing/Causing an Incident:

You could encounter a potential incident, one in process, or one to be carried out, at any time. You could also (intentionally or accidentally) cause an incident. You should react immediately. Do not try to handle it yourself.

If possible, do whatever you can to quickly gather evidence of what you are witnessing. Do not let this task interfere or slow down the reporting process. For example, you may want to write down peculiar system performances, error messages or other unusual behaviors.

Reporting a suspicion, incident, or virus:

Report all information security suspicions, incidents, or viruses as quickly as possible to your system coordinator. If problems and violations go unreported, they may lead to much greater losses for the organization than would have been incurred, had the problems been reported right away.

A Suspicion, an unconfirmed assumption of attack, is not yet an Incident. For this reason, it is even more critical to report a suspicion so as to avoid the incident from even happening or greatly decrease any negative results. It is the responsibility of every employee to do their part in detecting and reporting any possible incidents or suspicions You can make a difference by being aware of your environment, noticing unusual activities, safeguarding vulnerabilities, and quickly reporting any suspicions and/or incidents. If you are not sure if something unusual is a suspicion or not, it is best to report it and have the experts check it out. Remember, reporting a suspicion can prevent an incident.

Be suspicious of all e-mail file attachments, including those that appear to come from a trusted source.

Never execute file attachments directly from within e-mail. Use the e-mail program's Save It To Disk, manually scan the file with anti-virus software and open the file directly from the appropriate application.

If you are unsure about an e-mail attachment, delete it and contact the sending party for clarification. Ask yourself, does this person usually send e-mail attachments?

Ensure you have virus protection software active and scanning your PC periodically.

The greatest danger with computer viruses is that if it goes unreported and is not contained, it will continue to spread. Computer viruses can spread quickly and need to be eradicated as soon as possible to limit serious damage to computers and data.